REMARKS

Please find enclosed a new set of formal drawings to meet the Examiner's rejection of the drawings.

The Examiner objected to claims 3 and 4 on the ground of some minor deficiencies such as spelling errors. Since all of claims 1-5 have been cancelled, and news claims 6-10 have been substituted, these rejections should be obviated.

The Examiner rejected claims 1-5 as anticipated by the Provino patent (US 6,557,037). While this rejection has been obviated by cancellation of claims 1-5, new claims 6-10 are basically heavily amended versions of original claims 1-5 and so the undersigned will point out why the new claims distinguish over the Provino patent. The amendments should be assumed to have been made to improve the accuracy and clarity of expression of the invention and not to distinguish over Provino, unless language specifically identified in the argument below as distinguishing Provino was either added to the original claims or deleted from the original claims in making these new claims.

First, let's start with a high level overview of what the invention is and how it operates. The invention is basically a **performance tuned** virtual private network over the internet. The difference over prior art VPNs is that, in the inventions, a path through the internet is used which has been preplanned and pretested by specially selected ISP or ISX providers of routing and connectivity services. The path is planned to have a high bandwidth, low latency, low hop count characteristics which gives it improved and sustained improved performance over any randomly routed path through the internet.

The invention functions in an environment having a set of computers coupled to a LAN at a source site and a set of computers coupled to a LAN at a destination site. The idea is to use the internet to securely send data packets from computers at the source site to computers at the destination site over the internet without bandwidth bottlenecks or excessive delays which are inherent in internet operations. Security is provided by provision of a firewall/virtual private network (VPN) circuit at each end which creates a virtual private network tunnel over the internet between the two ends. However, computers at the source site may also want to send packets to servers on the internet at P addresses other than at the destination site. The idea is to provide a stable and efficient transport path across the internet between **AlterWAN**[1]tm configured destinations. This is done by taking P packets from computers at the source site and addressed to computers at the destination site and encapsulate them as the payload section of another P packet (tunneling) which has its destination address as the untrusted port (internet side) of the firewall at the destination site. The payload section of this second P packet (the original P packet) is then encrypted by the firewall/VPN circuit and sent to the firewall/VPN circuit at the other end where the encapsulated P packet is decrypted. This second P packet is called an AlterWAN packet and it gets created when the source site firewall/VPN recognizes the destination address of an P packet from a computer at the source site is an P address of a computer at the destination site. When the destination address of a packet from a computer at the source site is not an IP address of a computer at the destination site, it is not an AlterWAN packet. As a result, the firewall/VPN circuit does not encapsulate it in another IP packet and encrypt the payload. Therefore, an "AlterWAN destination" means a computer at the destination site, and "not an AlterWAN packet" means the packet is not addressed to an IP address of a computer at the destination site.

The key thing to note is that once the AlterWAN packet is generated, it is routed across the internet over a preplanned, pretested, low hop count, high bandwidth data path by specially selected ISP/ISX providers who have been selected and whose routers are configured to make sure AlterWAN packets get routed specially over this high bandwidth, low hop count path. All the new claims have been writen to specify that the ISP are selected in this way and provide a low hop count, high bandwidth path for AlterWAN packets. As used in the claims AlterWAN packets means packets which have other packets as their payloads and which have their payloads encrypted based upon whether the destination address of the original packet which was encapsulated in the second packet was addressed to an AlterWAN destination or not. The destination address of an AlterWAN packet is the IP address of the edge router of a local area network to which one or more computers at the destination end of the tunnel are coupled (or just a router or VPN circuit coupled to a computer).

The tunneling part is what provides the security and is known in the prior

[1] AlterWAN is a trademark of AlterWAN, Inc. All subsequent uses of the mark whether as a noun or not are to be understood as trademark uses.

art as virtual private networks. We are not claiming virtual private networks standing alone. The heart of the invention lies in the specially selected ISPs and how they recognize AlterWAN packets (by their destination addresses) and how these ISPs route and treat AlterWAN packets differently by routing them over a preplanned, pretested, low hop count, low latency, high bandwidth data path across the internet. It is this routing on the low latency, high bandwidth data path which dramatically improves performance over the prior art VPN tunnels. Although it is true that standard tunneling and encryption are used as part of the invention to provide privacy, that is not the whole invention. The VPN prior art does not do anything to reduce hop count or assure that the VPN packets travel only on high bandwidth, low latency paths.

The new claims speak in terms of firewalls with trusted and untrusted ports, AlterWAN packets and ISPs or ISXs. To clarify the meaning of trusted and untrusted ports, new claim 9 has been written so that the phrase "said source firewall having an untrusted port" appears at the beginning of step 3. A firewall has an untrusted port that is coupled to a WAN such as the internet and a trusted port which is coupled to devices on a local area network usually through a cable modem or other modem. Claim 9 has been written to specify. that the untrusted port is coupled to the first ISX/ISP provider on the internet and the trusted port is coupled to local devices at the source destination.

The term untrusted port appears for the first time in the original claims as filed, and is not in the specification, but persons skilled in this art know that firewalls have an untrusted port and a trusted port. At page 5, line 28 of the specification, the use of firewalls in the AlterWAN network is taught as follows:

> For example, if a customer site in San Jose needs to have AlterWAN service to another site in Tokyo, a "private tunnel" is built in each direction through the internet and two dedicated local loops, one at each end are established to connect the two customer sites to the first and last participating ISX providers in the private tunnel. Data security is implemented by the use of conventional or custom firewall/VPN technology. At each customer site, a firewall/VPN device is configured to securely encrypt the payload of each AlterWAN packet to be sent through a "private tunnel" to the far end customer site where the payload is decrypted.

Page 11, line 26 however is the beginning of a more informative passage which teaches which sides of the firewalls at each end of the private tunnel are the trusted and untrusted sides:

> More specifically, at each end of a private tunnel, a packet addressed to any of the IP addresses of devices at the other end of a private tunnel are recognized as packets that need to be converted to AlterWAN packets, encrypted by the firewall and encapsulated in another IP packet having as its destination address the IP address of the untrusted side of the firewall at the other end of the private tunnel. The composite AlterWAN packet is comprised of the encrypted original IP packet with an AlterWAN packet header which has as its destination address the IP address of the untrusted side of the destination firewall. At the firewall at the other end, these incoming AlterWAN packets will recognized because their destination addresses match the IP address of the untrusted side of the firewall. The firewall then strips off the AlterWAN packet header of the encapsulating packet and decrypts the original IP packet that was encapsulated using the same encryption algorithm and key or keys that were used to encrypt it. The decrypted packet then has an IP packet header which has a destination address which matches the IP address of some device on the LAN on the trusted side of the destination firewall. The decrypted packet is then put on the destination LAN and makes its way to the device to which it was addressed.

To clarify the meaning of this passages from the specification, the actual content of the AlterWAN packet is the same as any IP packet so the conversion process is really one of converting an IP packet that is addressed to an AlterWAN destination address into another IP packet which is addressed to the firewall at the other end of the AlterWAN tunnel and which has an encrypted payload which is the original IP packet. There is nothing unique in the AlterWAN IP packet itself except its destination address and even that is a conventional IP address. However, the destination address signals that a packet is an AlterWAN packet when it happens to be a specific IP address at an AlterWAN destination site (the IP address of the firewall at the other end of the AlterWAN VPN tunnel's high bandwidth, low latency, low hop count data path). This destination address tells the routers at the specially selected ISPs to route the AlterWAN packets along a low hop count, low latency, high bandwidth data path which has bee preplanned and pretested for AlterWAN packets. It is this special routing that vastly improves the performance over prior art VPN tunneling technology. In other words, the ISPs have been specially selected to have high bandwidth, low latency, low hop count data paths available to route AlterWAN packets on, and the routing tables of these ISPs have been configured to recognize AlterWAN packets and route them onto the high bandwidth, low latency, low hop count path (the preferential path). Other IP packets not addressed to the AlterWAN firewall at the other end of the tunnel are not routed along this preferential path.

In the process of reviewing claim 4, it was noted that certain steps are out of chronological order. Thus, new claim 9 has been written to put the steps in proper chronilogical order. Specifically, new steps 3, 4 and 5 are relocations of original steps 5 and 7 in claim 4, and the addition of a new step 3 to contract with all participating ISX/ISP providers to provide the preplanned, low hop count, high bandwidth routes which AlterWAN packets will travel. The idea is to look at all the available ISX/ISP providers which could possibly route AlterWAN packets between the source site and destination site and pick only the ones who will minimize the hop count and who will guarantee that the average available bandwidth on the data paths the AlterWAN packets will travel substantially exceeds the worst case bandwidth between the source and destination sites that the customer might consume. The specification includes the following teachings relevant to the contracting steps.

From Page 5, line 17

> Another key characteristic that all species within the genus of the invention will share is the transmission of secure encrypted data along preplanned high bandwidth, low hop-count routing paths between pairs of customer sites that are geographically separated. The encrypted AlterWAN data is sent through a high bandwidth, dedicated local loop connection to the first participating AlterWAN ISX/ISP facility. There, the AlterWAN packets are routed to the routers of only preselected ISX facilities on the internet. The preselected ISX/ISP facilities are ones which provide high-bandwidth, low hop-count data paths to the other ISX/ISP facilities along the private tunnel. The routers of these participating ISX/ISP facilities are specially selected to provide these high-bandwidth, low hop-count data paths either by their natural routing tables or by virtue of special routing tables that these ISX/ISP providers establish to route AlterWAN packets through high-bandwidth, low hop-count paths and route other internet traffic along other paths. ....

From Page 6, line 17

> This preplanning of the routing path causes traffic from AlterWAN™ customers to be transmitted quickly and without delay from end to end and not

experience delays due to lack of bandwidth or excessive hop count. Because the packet payload is encrypted, the data is secure during its transport across the internet through the "private tunnel". The AlterWAN™ network design minimize the number of hops each AlterWAN™ network packet experiences in its travel from source to destination thereby reducing latency by causing AlterWAN™ network traffic to be routed only over high bandwidth lines coupling participating ISX/ISP providers. Recently, there has been a large amount of building of ISX internet providers having fiber optic data paths to other providers to provide large amounts of bandwidth. Typically, one or both of the routers at the source and destination of the AlterWAN™ network can be co-located at the first ISX.

From page 15, line 18:

AlterWAN designers pretest these routes by performing a minimum of a ping test and traceroute test to verify the path data that AlterWAN packets will take through the private tunnel that is to be implemented as an AlterWAN connection.

This means testing is performed to make sure that the AlterWAN packets will be routed specially along a low latency, high bandwidth, low hop count data path.

The contracting steps of steps 4, 5 and 6 of new claim 9 are to make contracts with the ISX/ISP providers which can guarantee the low hop count and high bandwidth for AlterWAN packets. These are human steps so the overall claim amounts to a method of doing business to provide inexpensive virtual private WAN connectivity using the internet. A new pretesting step has been added to verify the ISPs selected in step 2 actually deliver what they promised. **Overall, new claim 9 is a process to build a high speed, private WAN to carry AlterWAN packets using the internet as the backbone generally by picking ISPs, testing them, making contracts, and installing routers and firewalls which are properly configured to route AlterWAN packets across high speed, high bandwidth, low latency, low hop count data paths. The only difference between an AlterWAN packet and a regular IP packet is that the destination IP address of the outer IP packet is the IP address of the untrusted port of the firewall at the other end of the Virtual Private Network tunnel or one of the other IP addresses that have been agreed upon by the selected ISP and ISX partners to be recognized and routed specially along the low hop count, low latency, high bandwidth data path. Also, with an AlterWAN packet, the payload section is actually another IP packet which has been encrypted. Like all other IP packets, an**

AlterWAN packet has a header and a payload section.

Steps 3, 5 and 7 of new claim 9 have been writtent to make them more clear than the original claim 4. Step 3 is directed to the processing done by the source site firewall/VPN circuit to receive IP packets from source site computers and determine if they are AlterWAN or not AlterWAN packets and to receive AlterWAN packets from the destination firewall. A packet received at the source site firewall from a source site computer is deemed to be an AlterWAN packet if it has as its destination address the IP address of any computer at the destination site (note that there is no limitation that the IP destination address be the IP address of the untrusted port of the firewall at the AlterWAN destination site). If the destination address is not one of the IP addresses at the AlterWAN destination site, the packet is deemed to be a non AlterWAN packet. If it is a AlterWAN packet, the IP packet transmitted from the source site computer is put into the payload section of a second IP packet and encrypted. The second IP packet is called the AlterWAN packet and has a header which includes as the destination address the IP address of the untrusted port of the destination site firewall. The untrusted port of both the source firewall and the destination firewall is the port coupled to the internet and are the endpoints of the VPN tunnel. The trusted port is the side connected to the LAN. For incoming IP packets, the source firewall receives them at its untrusted side and looks at the destination address for each to determine if the packet is addressed to the untrusted side of the source firewall. If so, the incoming packet is an AlterWAN packet. If not, it is not an AlterWAN packet. For AlterWAN packets, the AlterWAN header is stripped and the payload section is decrypted to recover the original IP packet. That original IP packet is then put on the LAN for sending to the computer to which the original IP packet is addressed.

Steps 5 and 7 have been moved to reflect the chronological order of steps in building a network and what they mean has been explained above. What they mean is a human contracts with a provider of local loop service to provide a local loop connection to the source and destination ISX/ISP provider to connect the routers at the source and destination sites to the ISX/ISP provider.

Anticipation Rejection

Claims 1-5 were rejected as anticipated by the Provino patent (US 6,5576,037).

The way the invention works is as follows. At a customer source site there are one or more computers, a source firewall and a source router. At a customer destination site there are one or more computers, a destination firewall and a destination router. A virtual private network tunnel through the internet is set up between the IP address of the firewall at the source and the IP address of the firewall at the destination.

The way the firewalls work is important. What the source firewall does is examine the destination addresses of IP packets arriving from the source site computers. If the destination address of a packet is the IP address of any of the computers at the destination site, the packet is encapsulated into the payload section of another IP packet. That IP packet has its destination address set to the IP address of the destination firewall and is called an AlterWAN packet. Its payload section only is then encrypted using an encryption algorithm and key known to the destination firewall. The AlterWAN packet is then sent on its way. Any IP packets that do not have as their destination address the IP address of a computer at the destination site are just sent on their way without encapsulation in another packet and without encryption. They are routed to whatever URL they are addressed to.

The source router routes the AlterWAN packets to a first ISP/ISX which has been specially selected and contracted with to have its routers recognize AlterWAN packets and route them through high bandwidth, low latency, low hop count data paths through the internet to other specially selected and contracted with ISP/ISX providers which do the same thing to AlterWAN packets.

Incoming IP packets at the destination firewall are inspected to determine which ones have as their destination addresses the IP address of the destination firewall. Any that have this destination address are deemed to be AlterWAN packets and have their payload sections decrypted to recover the original IP packet encapsulated therein. This packet is then routed to whatever computer at the destination site to which it was originally addressed.

The destination firewall works the same way for packets arriving from destination site computers and addressed to source site computers, but in reverse. The destination firewall encapsulates any IP packets addressed to a source site computer into an AlterWAN IP packet having as its destination address the IP address of the source firewall. Any other IP packet is just sent on its way. As previously described, incoming IP packets are recognized as AlterWAN packets if their destination addresses are the IP address of the destination firewall and are decrypted to recover the encapsulated IP packet. The recovered IP packet is then sent to whatever computer at the destination site to which it was originally addressed. Incoming IP packets not addressed to the destination firewall are just routed to whatever destination site computer to which they are addressed.

A key factor in the structure of the invention is who the ISX and ISP partners are that route the AlterWAN packets through the internet along the VPN tunnel created by the source and destination firewalls. They are ISPs who promise to deliver data paths with a low hop count, low latency and which has an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets travelling between the source site computers and the destination site computers. The data paths provided by these selected ISP/ISX providers are verified by pretesting to confirm that they actually deliver what was promised, and, if they do, the ISP/ISX is contracted with. The ISX and ISP partners agree to provide special treatment of AlterWAN packets that are to be sent between AlterWAN enabled locations. The ISX and ISP partners recognize these packets by the agreed upon IP destination addresses.

This preplanning of the route and selection of only the ISP and ISX partners that deliver high bandwidth, low latency, low hop count data paths and the agreement to provide preferential treatment to AlterWAN IP addressed packets being sent between AlterWAN enabled sites effectively pre-greases the skids so that AlterWAN packets zing through the tunnel very rapidly without the delays typically associated with other non AlterWAN IP packets bouncing around from router to router on the internet. This selection of ISPs and testing to verify they can do what they promise solves a long standing Quality of Service problem with the internet.

Prior art virtual private networks suffer from: unstable bandwidth, ISP traffic congestion, ISPs with limited capability, traffic re-routing based on factors out of the customer's control, potential to have additional monthly costs which are unpredictable imposed, and delays which are unpredictable because the traffic has no specific, pre-planned route to travel between corporate locations.

The prior art Provino patent does not teach this structure or this method of operating and it does not teach how to build such a high performance private WAN using the internet as a backbone.

The Provino patent discusses a means of facilitating resolution of secondary addresses. It discusses LAN, WAN and firewalls and the associated VPN and tunnels, but **importantly,** it does not discuss quality of service or any means of addressing and solving the quality of service issues that VPNs that use the internet as the backbone suffer from. No mention is made in Provino of choosing ISPs who promise and deliver low hop count, high bandwidth data paths. Reference 2 goes into detail about VPNs, but VPNs are only part of the AlterWAN solution.

The real crux of the invention is how VPNs are implemented using carefully selected and tested ISPs who provide low hop count, high bandwidth data paths so as to provide a low-cost, private, high performance wide area network using the internet as a backbone. Provino does not recognize this problem nor provides its solution.

New claim 6 includes the following element not taught in Provino:

> one or more routers of other participating ISX/ISP providers of internet services besides said source ISX/ISP provider including a router at an endpoint participating ISX/ISP provider, said routers of said source and endpoint ISX/ISP providers and said other participating ISX/ISP providers functioning to implement a predetermined private tunnel data path for said AlterWAN packets coupling a router of said source ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP providers and said other ISX/ISP providers being providers of internet services who have contracted to provide and who have been pretested to verify that they do in fact provide a low hop count portion of a data path between said source site and said destination site for said AlterWAN packets with an average available bandwidth along said portion of said data path travelled by said AlterWAN packet which each ISX/ISP provider provides which substantially exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site;

New claim 7 includes the following process element not taught in Provino:

> at said source router, converting both said AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated local loop connection coupling said source router to a specially selected source participating ISX/ISP provider and transmitting said signals to said specially selected source participating ISX/ISP provider, said specially selected source participating ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop-count data paths to next participating ISX/ISP provider in said virtual private network or because the routing tables of the router of said specially selected source participating ISX/ISP

provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said virtual private network and wherein said source participating ISX/ISP provider and all other participating ISX/ISP providers whose routers route AlterWAN packets have contracted to provide a data path for said AlterWAN packets with an average available bandwidth which exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site of said customer.

New claim 8 includes the following element which is not taught in Provino.

> a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said router and channel service unit functioning to receive said AlterWAN packets and said conventional packets from said first firewall circuit and convert said packets into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN packets and conventional packets over said dedicated data path to said specially selected first participating ISX/ISP provider where said AlterWAN packets will be routed via said virtual private network tunnel and specially selected participating ISX/ISP providers to said second firewall and non-AlterWAN packets will be routed along paths on the internet other than said virtual private network tunnel and wherein said first participating ISX/ISP provider and all said other ISX/ISP providers are providers who have contracted to and do in fact provide data paths for AlterWAN packets which combine to form a low hop count data path with an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site.

New claim 9 includes the following method step which is not taught in Provino:

> 2) examining available ISX/ISP internet service providers that can route AlterWAN packets between said source and destination sites and selecting two or

> more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which AlterWAN packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made so as to minimize the number of hops on the internet the routers at participating ISX/ISP providers will cause AlterWAN packets to take while traveling between said source and destination sites and so as to guarantee that the average available bandwidth of the data paths along which said AlterWAN packets traveling between computers at said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites;

New claim 10 has the following element which is not disclosed in the Provino patent:

> one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement a low hop count data path in the form of a virtual private network tunnel through the internet coupling one or more devices at said customer source site to one or more computers at said customer destination site, said low hop count data path having an average available bandwidth which is substantially greater than the worst case bandwidth consumption of AlterWAN packets traveling between said customer source site and said customer destination site;

The Examiner cites to Provino Col. 9 and Col. 10 as evidence that it was known in the prior art to provide a predetermined private tunnel data path from a first ISX/ISP through participating ISX/ISP providers to an endpoint participating ISX/ISP. The pertinent Provino teachings are as follows:

> Generally, the virtual private network 15 is maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14, but which also desires to limit access to the servers 31(s) by devices 12(m) and other devices over the Internet 14 in a controlled manner. The firewall 30 serves to control access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15. In that

operation, the firewall 30 also connects to the Internet 14, receives message packets therefrom for transfer to a server 31(s). If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). The firewall may be similar to other devices 31(s) in the virtual private network 15, with the addition of one or more connections to the Internet, which are generally identified by reference numeral 43.

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm and key that it (that is device 12(m)) will use to the firewall 30 during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel. Thereafter, the device 12(m) and firewall 30 can transfer message packets over the secure tunnel. The device 12(m), in generating message packets for transfer over the secure tunnel, makes use of the secure packet processor 26 to encrypt the portions of the message packets which are to be encrypted prior to transmission by the network interface 21 to the ISP 11 for transfer over the Internet 14 to the firewall 30, and to decrypt the encrypted portions of the message packets received by the device 12(m) which are encrypted. In particular, after the packet generator 22 generates a message packet for transmission to the firewall 30 over the secure tunnel, it will provide the message packet to the secure packet processor 26. The secure packet processor 26, in turn, encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key. After the firewall 30 receives a message packet from the device 12(m) over the secure tunnel, it will decrypt it and, if the intended recipient of the message packet is another device, such as a server 31(s), in the virtual private network 14, it (that is, the firewall 30) will transfer the message packet to that other device over the communication link 33.

For a message packet that is to be transferred by a device, such as a server 31(s), in the virtual private network 15 to the device 12(m) over the secure tunnel, the firewall 30 will receive such to the message packet over the communication link 33 and encrypt the message packet for transfer over the Internet 14 to the ISP 11. The ISP 11, in turn, forwards the message packet to the device 12(m), in particular to its network interface 21. The network interface 21 provides the message packet to the secure packet processor 26, which decrypts the encrypted portions of the message packet, using the decryption algorithm and key.

A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that nameserver 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Thus, the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(s) which is to be accessed from that nameserver 17.

To accommodate this problem, when the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween, in addition to possibly providing the device 12(m) with the identifications of the encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel, the firewall 30 also provides the device 12(m) with the identification of a nameserver, such as nameserver 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). The identification of nameserver 32 is also stored in the IP parameter store 25, along with the identification of nameserver 17 which was provided by the ISP 11 when the device 12(m) logged on to the ISP 11 at the beginning of a communications session. Thus, when the device 12(m) is to transmit a message packet to a device, such as a server 31(s) in the virtual private network 14 using a human-readable Internet address provided by, for example, an operator, the device 12(m) will initially access the nameserver 17, as described above, to attempt to obtain the integer Internet address associated with the human-readable Internet address. Since nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m), it will send a response message packet so indicating. The device 12(m) will thereafter generate a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message packet provided by the

> device 12(m), it will provide the integer Internet address in a manner that is generally similar to that described above in connection with nameserver 18, except that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m). In the message packet transmitted by the firewall 30, it will be appreciated that the integer Internet address in the message packet will be in the data portion of the message packet transferred over the secure tunnel and, accordingly, will be in encrypted form. The message packet will be processed by the device 12(m) in a manner similar to that described above in connection with other message packets received by it over the secure tunnel, that is, the message packet will be decrypted by the secure packet processor 26 prior to being provided to the packet receiver and processor 23 for processing.

Careful study of these passages indicates that the notion of providing a virtual private network through the internet is known. However, doing so using specially selected ISPs whose routers are set up to recognize AlterWAN packets and route them through predetermined low latency, low hop count data paths which have an average available bandwidth which greatly exceeds the worst case traffic scenario and which have been pretested to verify this is not taught in any of these passages. That is what is generally being claimed in all the new claims in various forms of expression. It is this data path through the internet which gives the VPN of the invention its terrific performance advantage.

Accordingly, the applicant believes the new claims distinguish over Provino.

Respectfully submitted,

Dated: June 10, 2004

Ronald C. Fish

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.
on 6/10/04

(Date of Deposit)

Ronald C. Fish

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843